

U skladu sa eIDAS-om i kvalifikovanom Uslugom validacije

Politika kvalifikovane validacije elektronskog potpisa i elektronskog pečata

Verzija 1.2

Sadržaj

Sadržaj 2

1 Uvod 6

1.1 Pregled 6

1.2 Naziv dokumenta i identifikacija 6

1.2.1 Efekat 6

Obim predmeta 6

Vremenski obim 7

Lični obim **Error! Bookmark not defined.**

Geografski obim 7

1.3 PKI učesnici 8

1.3.1 Autoriteti za sertifikaciju 8

1.3.2 Pretplatnici 8

1.3.3 Oslanjajuće strane 8

1.4 Uprava za politiku 8

1.4.1 Organizacija koja administrira dokument 8

1.4.2 Kontakt osoba 8

1.4.3 Osoba ili organizacija odgovorna za prikladnost izjave o praksi za politiku validacije 9

1.4.4 Procedure odobravanja izjave o praksi 9

1.5. Definicije i akronimi 9

1.5.1. Definicije 9

1.5.2. Akronimi 12

2 Odgovornosti za objavljivanje i skladištenje 14

2.1 Skladišta 14

2.2 Vreme ili učestalost objavljivanja 14

2.2.1 Učestalost ojavljivanja odredbi i uslova 14

2.3 Komponente usluge validacije potpisa 15

2.3.1 Akteri službe za validaciju potpisa 15

2.3.2. Arhitektura servisa 15

2.4 Politike i prakse 16

2.4.1 Organizacija koja administrira dokumentaciju Pružaoca usluga od poverenja 16

2.4.2 Kontakt osoba 16

2.4.3 Primenljivost dokumentacije Pružaoca usluga poverenja 16

3 Zahtevi / izjave o tehničkim mehanizmima i primeni standarda 17

3.1. Tehnički pandani Politike usluge validacije 17
3.1.1. Pristup vremenu potpisivanja 17
3.1.2. Definisanje kvalifikovanog statusa potpisa ili pečata 18
3.2. Ulazna i izlazna ograničenja za procedure kreiranja, povećanja i validacije potpisa 19
3.2.1. Ulazna ograničenja koja će se koristiti prilikom generisanja, povećanja i/ili validacije potpisa u kontekstu identifikovane politike potpisa 19
Vreme validacije 19
Proces validacije 20
3.2.3. Izlazna ograničenja koja će se koristiti za generisanje / povećanje potpisa u kontekstu identifikovane politike potpisa 20
4 Tehničke mere bezbednosti 21
4.1 Sigurnosne garancije 21
4.2 Mere predostrožnosti za računarsku bezbednost 21
4.3 Tehničke mere predostrožnosti vezane za životni ciklus 21
4.4 Redovna sertifikacija 22
4.5 Kontinuirano praćenje tehnologije 22
4.6 Prihvatanje Pružaoca sertifikata i vremenskog žigosanja 22
4.7 Dostupnost određenih elemenata usluge validacije 23
5 Kontrole objekata, upravljanje i rada 24
5.1 Fizičke kontrole 24
5.1.1 Lokacija i izgradnja 24
5.1.2 Fizički pristup 24
5.1.3 Napajanje i klimatizacija 25
5.1.4 Izloženost vodi 26
5.1.5 Prevencija i zaštita od požara 26
5.1.6 Skladištenje medija 26
5.1.7 Odlaganje otpada 26
5.1.8 Rezervna kopija van lokacije 27
5.2 Proceduralne kontrole 27
5.2.1 Povereničke uloge 28
5.2.2 Broj potrebnih osoba po zadatku 28
5.2.3 Identifikacija i autentifikacija za svaku ulogu 29
5.2.4 Uloge koje zahtevaju razdvajanje dužnosti 29
5.3 Kontrola osoblja 29
5.3.1 Zahtevi za kvalifikacije, iskustvo i odobrenje 30
5.3.2 Procedure provere pozadine 30

5.3.3 Zahtevi za obuku 31
5.3.4 Učestalost i uslovi prekvalifikacije 31
5.3.5 Učestalost i redosled rotacije poslova 31
5.3.6 Sankcije za nedozvoljene radnje 31
5.3.7 Zahtevi nezavisnog izvođača 32
5.3.8 Dokumentacija dostavljena osoblju 32
5.4 Procedure evidentiranja revizije 32
5.4.1 Vrste snimljenih događaja 33
5.4.2 Učestalost obrade dnevnika revizije 36
5.4.3 Period zadržavanja za evidenciju revizije 36
5.4.4 Zaštita dnevnika revizije 36
5.4.5 Procedure za pravljenje rezervnih kopija dnevnika revizije 37
5.4.6 Sistem prikupljanja revizije (interni naspram eksternog) 37
5.4.7 Obaveštenje subjektu koji izaziva događaj 37
5.4.8 Procene ugroženosti 37
5.5 Kompromitovanje i oporavak od katastrofe 38
5.5.1 Procedure za rukovanje incidentima i kompromitovanjem 38
5.5.2 Računarski resursi, softver i/ili podaci su oštećeni 38
5.5.3 Mogućnosti kontinuiteta poslovanja nakon katastrofe 38
5.6 Prestanak usluge validacije 39
6 Tehničke bezbednosne kontrole 40
6.1 Zaštita privatnog ključa i inženjerske kontrole kriptografskog modula 40
6.1.1 Standardi i kontrole kriptografskog modula 40
6.1.2 Privatni ključ (N od M) Kontrola više osoba 41
6.1.3 Deponovanje privatnog ključa 41
6.1.4 Rezervna kopija privatnog ključa 41
6.1.5 Arhiviranje privatnog ključa 41
6.1.6 Prenos privatnog ključa u ili iz kriptografskog modula 41
6.1.7 Skladištenje privatnog ključa na kriptografskom modulu 42
6.1.8 Način aktiviranja privatnog ključa 42
6.1.9 Metoda deaktiviranja privatnog ključa 42
6.1.10 Metoda uništavanja privatnog ključa 42
6.1.11 Ocena kriptografskog modula 42
6.2 Podaci o aktivaciji 43
6.2.1 Generisanje i instalacija aktivacionih podataka 43
6.2.2 Zaštita podataka aktivacije 43

6.2.3 Drugi aspekti aktivacionih podataka 43
6.3 Kontrole kompjuterske bezbednosti 43
6.3.1 Specifični tehnički zahtevi za bezbednost računara 43
6.3.2 Ocena računarske bezbednosti 44
6.4 Tehničke kontrole životnog ciklusa 44
6.4.1 Kontrole razvoja sistema 44
6.4.2 Kontrole upravljanja sigurnošću 45
6.4.3 Sigurnosne kontrole životnog ciklusa 45
6.5 Kontrole mrežne bezbednosti 46
6.6 Vremensko žigosanje 47
7 Revizija usklađenosti i druge procene 47
7.1 Učestalost ili okolnosti procene 48
Pružalac usluge validacije će izvršiti ocenu usaglašenosti svake godine. 48
7.2 Identitet/Kvalifikacije procenjivača 48
7.3 Odnos procenjivača prema procenjenom entitetu 48
7.4 Teme obuhvaćene ocenjivanjem 48
7.5 Radnje preduzete kao rezultat nedostatka 49
7.6 Saopštavanje rezultata 49
REFERENCE 50

1 Uvod

Ovaj dokument sadrži Politiku usluge validacije kvalifikovanih elektronskih potpisa i elektronskih pečata koju je definisala i kojom upravlja Inception d.o.o Beograd (u daljem tekstu: Inception ili Pružalac usluga validacije) u vezi sa Uslugom validacije.

Politika za uslugu validacije kvalifikovanih elektronskih potpisa i elektronskih pečata je u skladu sa zahtevima postavljenim eIDAS Uredbom [1], evropskim standardom ETSI EN 319 401 [2], usluga koja se pruža u skladu sa ovim propisima je Usluga validacije.

1.1 Pregled

Politika za validaciju usluge za kvalifikovane elektronske potpise i elektronske pečate (u daljem tekstu: Politika validacije) je skup pravila koja specificiraju upotrebljivost usluge validacije za zajednicu i/ili klasu aplikacija sa zajedničkim bezbednosnim zahtevima.

Politika validacije postavlja osnovne zahteve za pružaoca usluga validacije u vezi sa kvalifikovanom validacijom koju treba uspostaviti.

Politika validacije je jedan od nekoliko dokumenata koje izdaje Pružalac usluge validacije koji zajedno regulišu uslove usluga koje pruža Pružalac usluge validacije. Ostali važni dokumenti uključuju Praktična pravila za uslugu validacije kvalifikovanih elektronskih potpisa i elektronskih pečata i druge ugovore sa klijentima i partnerima.

1.2 Naziv dokumenta i identifikacija

Izdavač	
Naziv dokumenta	Inception d.o.o Beograd U skladu sa eIDAS-om i kvalifikovanom Uslugom validacije Politika validacije
OID	1.3.6.1.4.1.57738.50.1.1.2.0
Verzija dokumenta	1.2
Datum stupanja na snagu 01.12.2022.	

1.2.1 Efekat

Praktična pravila validacije i Politika validacije zasnovanu na ovim politikama treba revidirati najmanje jednom godišnje i obezbediti njihovu dopunu potencijalno izmenjenim zahtevima i preduslovima.

Obim usluge

Politika validacije definiše specifične zahteve za usluge opisane u ovom dokumentu.

Vremenski okvir

Trenutna verzija Politike validacije je na snazi od datuma stupanja na snagu navedenog u odeljku 1.2 ovog dokumenta, do povlačenja. Efekat automatski prestaje po prestanku pružanja usluga ili pri izdavanju novije verzije Praktičnih pravila validacije.

Obim učesnika

Efekat Politike validacije se proteže na svakog od pomenutih učesnika.

Pružalac usluge validacije pruža usluge prvenstveno građanima Republike Srbije i organizacijama registrovanim u Republici Srbiji, ali ne isključuje građane ili organizacije iz drugih zemalja sve dok prihvataju sistem pravila kojih se pridržava Pružalac usluge validacije i kontrole. neophodno kako bi se pružene usluge mogle obavljati bezbedno i u skladu sa zakonom Republike Srbije.

Geografski obim

Trenutna Politika validacije zasnovana je na zahtevima Evropske unije, ali uključuje i zahteve specifične za Srbiju za usluge koje posluju u skladu sa srpskim zakonima u Republici Srbiji.

Pružalac usluge validacije može proširiti geografski obim usluge, u ovom slučaju neće koristiti manje stroge zahteve od onih koji se primenjuju u Politici validacije. U uslugama koje se pružaju stranim klijentima, detaljni uslovi koji se razlikuju od Politike validacije mogu se regulisati posebnim ugovorom o uslugama.

Usluga koja se pruža u skladu sa ovom Politikom validacije dostupna je širom sveta. Valjanost dokumenata, materijal za dugoročnu validaciju i pripadajuće izdate izjave arhiviraju se prema sadašnjoj Politici validacije.

Politika validacije je nezavisna od geografske lokacije sa koje su poslati u arhivu i odakle se isčitavaju.

Usluga koja se pruža u skladu sa ovom Politikom validacije može se koristiti samo na način opisan u ovoj Politici validacije i Praktičnim pravilima validacije.

1.3 PKI učesnici

1.3.1 Autoriteti za sertifikaciju

Inception d.o.o (Pružalac usluga) je Pružalac usluga od poverenja, u okviru kojeg se Usluga poverenja bavi validacijom elektronskih potpisa, elektronskih pečata, vremenskih žiga i njihovih autorskih sertifikata, opciono uključujući i validaciju potpisanog i zapečaćenog elektronskog dokumenta.

1.3.2 Pretplatnici

Pretplatnici definišu obim korisnika koji koriste uslugu, a pretplatnici pokrivaju i naknade za usluge koje se odnose na korišćenje ovih usluga.

1.3.3 Oslanjajuće strane

Oslanjajuća strana nije nužno u ugovornom odnosu sa Pružaocem usluga validacije.

1.4 Uprava za politiku

1.4.1 Organizacija koja administrira dokument

Podatke organizacije koja administrira Politiku validacije možete pronaći ovde:

Naziv organizacije	Inception d.o.o Beograd
Adresa organizaije	Admirala Vukovića 57, Beograd, Srbija
Telefon	+381 11 2920 355
Broj faksa	+381 11 2920 355
Email adresa	office@inception.rs

1.4.2 Kontakt osoba

Pitanja u vezi sa Politikom validacije mogu se direktno postaviti sledećoj osobi:

Kontakt osoba	Jovan Vistać
Naziv organizacija	Inception d.o.o Beograd
Adresa organizacije	Admirala Vukovića 57, Beograd, Srbija
Telefon	+381 11 2920 355
Broj faksa	+381 11 2920 355
Email adresa	office@inception.rs

1.4.3 Osoba ili organizacija odgovorna za usklađenost Praktičnih pravila sa Politikom validacije

Pružalac koji je Praktična pravila validacije odgovoran je za njegovu usklađenost sa Politikom validacije koja se u njoj pominje i za pružanje usluge u skladu sa propisima.

1.4.4 Procedure odobravanja Praktičnih pravila

Pružalac usluge validacije će opisati proceduru prihvatanja Praktičnih pravila validacije koja objavljuje njenu usklađenost sa ovom Politikom validacije u datim Praktičnim pravilima validacije.

1.5. Definicije i akronimi

1.5.1. Definicije

(Potpis) Vrsta obaveze	Indikacija tačne implikacije digitalnog potpisa koju potpisnik prihvata
Driving Application	Aplikacija koja koristi sistem za kreiranje potpisa da bi kreirala potpise ili aplikaciju za validaciju potpisa u cilju validacije digitalnih potpisa ili aplikaciju za povećanje potpisa radi povećanja digitalnih potpisa
eIDAS uredba	Uredba (EU) br. 910/2014 Evropskog parlamenta i saveta od 23. jula 2014. o elektronskoj identifikaciji i uslugama poverenja za elektronske transakcije na unutrašnjem tržištu i stavljanju van snage Direktive 1999/93/EC
Dokaz o postojanju	Dokaz koji dokazuje da je objekat postojao na određeni datum/vreme
	Aplikacija za validaciju

Aplikacija koja validira potpis u odnosu na politiku validacije potpisa, koja se sastoji od skupa ograničenja validacije i koja daje	indikaciju statusa (tj. status validacije potpisa) i izveštaj o validaciji potpisa
Politika validacije potpisa	Lista ograničenja koja obrađuje aplikacija za validaciju potpisa
Izveštaj o validaciji potpisa	Sveobuhvatan izveštaj o validaciji koji aplikacija za validaciju potpisa daje aplikaciji za vožnju i omogućava **aplikaciji za vožnju** da pregleda detalje odluka donetih tokom validacije i istražuje detaljne uzroke indikacije statusa koju obezbeđuje aplikacija za validaciju potpisa
Politika usluge provere potpisa	Skup pravila koja ukazuju na primenljivost usluge validacije potpisa na određenu zajednicu i/ili klasu aplikacije sa zajedničkom bezbednošću
Validacija potpisa	Proces verifikacije i potvrđivanja da je digitalni potpis tehnički validan
Usluga validacije potpisa	Sistem dostupan preko komunikacione mreže, koji potvrđuje digitalni potpis
Pretplatnik	Pravno ili fizičko lice koje je ugovorom sa Inception-om vezano za sve obaveze pretplatnika. U Inception ekosistemu, pretplatnici se sastoje i od kupaca (pružaoca usluga) koji su potpisali ugovor sa Inception-om kao krajnji korisnici koji su prihvatili samo odredbe i uslove usluga koje koriste
	Validacija kvalifikovanog elektronskog potpisa

Validacija kako je navedeno u Uredbi (EU) br. 910/2014 [i.1], član 32	
Validacija kvalifikovanih elektronskih pečata	Validacija kako je navedeno u Uredbi (EU) br. 910/2014 [i.1], član 40
Validacija	Proces verifikacije i potvrđivanja da je sertifikat ili digitalni potpis važeći
Oslanjajuće stranke	Fizičko ili pravno lice koje se oslanja na uslugu provere potpisa
Pružalac usluga	Prodavac koji pruža IT rešenja i/ili usluge krajnjim korisnicima i organizacijama
Pravila primenljivosti potpisa	Skup pravila, primenljivih na jedan ili više digitalnih potpisa, koji definišu zahteve za utvrđivanje da li je potpis pogodan za određenu poslovnu ili pravnu svrhu
Povećanje potpisa	Proces uključivanja informacija u digitalni potpis sa ciljem da se održi validnost tog potpisa na duži rok
Uređaj za kreiranje potpisa	Konfigurisani softver ili hardver koji se koristi za implementaciju podataka za kreiranje potpisa i za kreiranje vrednosti digitalnog potpisa
Aplikacija za validaciju potpisa	Aplikacija koja validira potpis u odnosu na politiku validacije potpisa, koja se sastoji od skupa ograničenja validacije i koja daje indikaciju statusa (tj. status validacije potpisa) i izveštaj o validaciji potpisa

Status validacije potpisa	UKUPNO-USPEŠNO, UKUPNO-NEUSPEŠNO ili NEODREĐENO
Verifikacija potpisa	Proces provere kriptografske vrednosti potpisa korišćenjem podataka za verifikaciju potpisa
Potpisnik	Osoba koja je kreator digitalnog potpisa

1.5.2. Akronimi

AdES	SVS
AdES/QC	TSP
	XAdES
ASiC	XML
BSP	SVC
CA	SVSP
Napredni elektronski potpis	SVSServ
Napredni elektronski potpis kreiran sa kvalifikovanim sertifikatom	
Associated Signature Container	**Driving Application**
Parametar poslovnog opsega	Elektronski potpisi i infrastruktura
Autoritet za izdavanje sertifikata	Onlajn protokol statusa sertifikata
DA	Identifikator objekta
ESI	Prenosivi format dokumenta Napredni
OCSP	elektronski potpis
OID	Infrastruktura javnog ključa
PAdES	Kvalifikovani elektronski potpis
	Kvalifikovani pružalac usluga od
PKI	poverenja
QES	Kvalifikovani uređaj za kreiranje potpisa
QTSP	Aplikacija za kreiranje potpisa
QSCD	Potpisani dokument
SCA	Potpisani objekat podatakaSecure Uređaj
SD	za kreiranje potpisa
SDO	Aplikacija za validaciju potpisa
SSCD	Izveštaj o validaciji potpisa
SVA	Usluga provere potpisa
SVR	Pružalac usluga od poverenja

XML Napredni elektronski potpis
eXtensible jezik za označavanje
Klijent validacije potpisa

Protokol usluge validacije potpisa
Server za proveru validacije potpisa

2 Odgovornosti za objavljivanje i skladištenje

2.1 Skladišta

Pružalac usluge validacije će objaviti ugovorne uslove i politike elektronskim putem na svojoj veb stranici.

Radna verzija novih dokumenata koji se uvode biće objavljena na internet stranici 30 dana pre stupanja na snagu.

Dokumenti koji su na snazi biće dostupni na sajtu pored svih prethodnih verzija svih dokumenata.

Stvarna verzija politika i ugovornih uslova biće čitljiva u korisničkoj službi Pružaoca usluge validacije.

Nakon zaključenja ugovora, Pružalac usluge validacije će učiniti pojedinačni Ugovor o usluzi, Opšta pravila, Politiku validacije i Praktična pravila validacije dostupnim Korisniku na trajnom mediju, ili na način koji može biti preuzeto od strane Korisnika.

Pružalac usluge validacije obaveštava svoje Korisnike o promeni Opštih uslova.

2.2 Vreme ili učestalost objavljivanja

2.2.1 Učestalost objavljivanja odredbi i uslova

Najvažniji uslovi za pružanje usluge sadržani su u ugovoru o uslugama koji Korisnik potpisuje prilikom zaključenja ugovora.

Pružalac usluge proverava Opšta pravila godišnje ili u slučaju izuzetnog zahteva za promenu sa prioritetom pregleda Opšta pravila i vrši neophodne izmene.

Dokument će i nakon najmanje izmene dobiti novi broj verzije, a uzimajući u obzir vreme potrebno za proces odobravanja, odrediće se i planirani datum stupanja na snagu.

Prihvaćeni dokument biće objavljen na veb stranici Pružaoca usluge validacije i biće poslat na uvid Ministarstvu trgovine, turizma i telekomunikacija 30 dana pre stupanja na snagu planiranog unosa.

Pružalac usluge validacije će prihvatiti komentare u vezi sa Opštim uslovima i odredbama objavljenim 14 dana pre njihovog stupanja na snagu, na kontakt podatke definisane u odeljku 1.41.

U slučaju zapažanja koja zahtevaju suštinske izmene, dokument će biti izmenjen. Pružalac usluge validacije će zatvoriti i objaviti verziju Opštih uslova i dopuna sa primedbama 7. dan pre stupanja na snagu.

2.3 Komponente usluge validacije potpisa

2.3.1 Akteri službe za validaciju potpisa

Poslovanje servisa za validaciju uključuje učešće:

- Klijent validacije potpisa (SVC)

  Softverska komponenta koja obezbeđuje korisnički interfejs za **driving application** koju koriste pretplatnici usluge eValidacije.

- **Driving Application** (DA)

  Aplikacija koja klijentu validacije potpisa obezbeđuje funkcionalnost validacije potpisa.

- Protokol usluge validacije potpisa (SVP)

  Bezbedan komunikacioni kanal za razmenu informacija sa Servisom za validaciju potpisa.

- Server za proveru validacije potpisa (SVSServ)

  Komponenta koja implementira protokol validacije potpisa na strani Pružaoca usluge provere potpisa.

- Aplikacija za validaciju potpisa (SVA)

  Softverska komponenta koja je odgovorna za validaciju potpisa, koja implementira algoritam validacije i kreira izveštaj o validaciji potpisa.

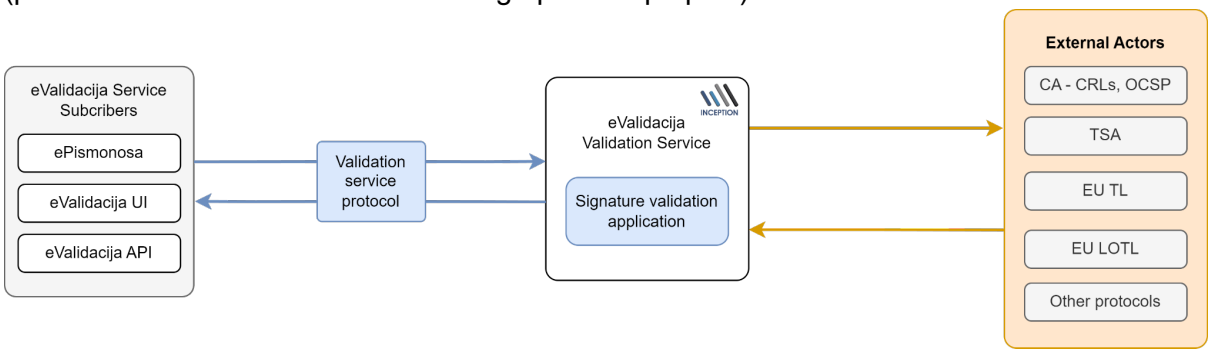
- Spoljni akteri

  Drugi izvori poverenja – Sertifikaciona tela, Tela za vremensko žigosanje, pružaoci evropskih pouzdanih lista, Evropska komisija koja obezbeđuje listu pouzdanih lista koje su pozvane da ispune svoju svrhu.

2.3.2. Arhitektura servisa

Server za proveru validacije potpisa (SVSServ) implementira aplikaciju za proveru validacije potpisa, odnosno aplikacija vrši verifikaciju formata, identifikaciju sertifikata potpisnika, kontekst validacije, Ks.509 validaciju, kriptografsku validaciju, prihvatanje potpisa (tj. zahteve za validaciju potpisa), prema ETSI TS 119 102-1 [3] specifikaciji.

Aplikacije za potpis/validaciju (DA) Inception-a se dele u klijentskom i serverskom režimu (preko Internet veze sa serverom usluge provere potpisa).



Slika 1 – Konceptualni režim validacije potpisa

2.4 Politike i prakse

2.4.1 Organizacija koja administrira dokumentaciju Pružaoca usluga od poverenja

PKI tim Inception je odgovoran za administraciju skupa praksi Inception usluga za validaciju.

2.4.2 Kontakt osoba

Inception d.o.o (Pružalac usluga) je Pružalac usluga poverenja, u okviru kojeg se Usluga poverenja bavi validacijom elektronskih potpisa, elektronskih pečata, vremenskih žigova i njihovih autorskih sertifikata, kao i validacijom prethodno navedenih.

Kontakt osoba	Jovan Vistać
Naziv organizacije	Inception d.o.o
Adresa organizacije	Admirala Vukovića 57, Beograd, Srbija
Telefon	+381 11 2920 355
Broj faksa	+381 11 2920 355
Email adresa	office@inception.rs

2.4.3 Primenljivost dokumentacije Pružaoca usluga poverenja

Politiku usluge validacije i pružanje usluga nadgleda Ministarstvo trgovine, turizma i telekomunikacija. Ministarstvo trgovine, turizma i telekomunikacija vodi registar o politici sertifikata i o pružaocima usluga validacije koji primenjuju ove politike.

Ova Politika usluge validacije je objavljena na korporativnoj veb stranici Inception-a na engleskom jeziku, što je zvanična verzija.

- https://inception.rs/ca/

3 Zahtevi / izjave o tehničkim mehanizmima i primeni standarda

3.1. Tehnički pandani Politike usluge validacije

Ova politika validacije će potvrditi elektronske potpise i naznačiti da li su napredni elektronski potpisi (AdES) ili AdES podržani kvalifikovanim sertifikatom (AdES/KC).
Svi sertifikati i njihovi povezani lanci koji podržavaju potpise su validirani od strane registra kvalifikovanih dobavljača usluga od poverenja (ovo uključuje sertifikat potpisnika i sertifikate koji se koriste za validaciju usluga statusa validnosti sertifikata – CRL, OCSP i vremenske oznake).

Da bi se utvrdila kvalifikacija sertifikata, Aplikacija za validaciju potpisa prati standardne elektronske potpise i infrastrukture (ESI); Politike potpisivanja; Deo 4: Politika validacije potpisa za evropske kvalifikovane elektronske potpise/pečate koji koriste pouzdane liste (ETSI TS 119 172-4). Analizira svojstva sertifikata i primenjuje moguća poništavanja sa povezane liste pouzdanih.

Pružalac usluge validacije će uvek izračunati status sertifikata za dva različita vremena: izdavanje sertifikata i vreme potpisivanja / validacije. Ovo je neophodno jer se kvalifikacija sertifikata može vremenom razvijati. Uredba o eIDAS-u jasno definiše ova različita vremena u članu 32 i povezanom Aneksu I.

3.1.1. Pristup vremenu potpisivanja

Vreme potpisivanja u odnosu na koje će se verifikovati validnost potpisa biće definisano na sledeći način:

1. Vreme potpisivanja će se pokušati definisati na osnovu dokaza o postojanju (npr. vremenske oznake ili evidencije dokaza) prisutnog u potpisu.

2. Ako takav dokaz postojanja nije dostupan (npr. iz potpisa se ne može izvući dokaz o postojanju), a aplikacija o funkcionalnosti je naznačila vreme koje treba koristiti kao vreme potpisivanja, koristiće se ovo vreme.

3. U nedostatku dokaza o postojanju i naznake iz aplikacije za funkcionalnost, vreme potpisivanja će biti postavljeno na vreme validacije (trenutno vreme).

3.1.2. Definisanje kvalifikovanog statusa potpisa ili pečata

Da bi se definisalo da li je potpis ili pečat Kvalifikovani elektronski potpis ili Kvalifikovani elektronski pečat sa privatnim ključem koji se nalazi u uređaju za kreiranje kvalifikovanog potpisa, sledeće provere će izvršiti Aplikacija za validaciju potpisa.

Definisanje liste pouzdanih usluga za sertifikat za potpisivanje ili pečat

Usluga validacije će proveriti da li se sertifikat za potpisivanje ili pečaćenje može vezati za listu poverenja koje je naznačeno u registru kvalifikovanih pružalaca usluga od poverenja. Da bi se to uradilo, registar će se redovno preuzimati i validnost će biti verifikovana (potpis na listi poverenja i istekom). Usluge poverenja definisane u ovoj listi će se zatim filtrirati prema osnovnom sidru sertifikata za potpisivanje/pečaćenje i biće verifikovano da je lanac poverenja navedeno sa ispravnim tipom usluge (Sertifikaciono telo za kvalifikovane sertifikate) i informacije o statusu usluge.

Definisanje kvalifikovanog statusa sertifikata za potpisivanje ili pečat

Da bi se proverilo da li je sertifikat za potpisivanje ili pečatiranje, Kvalifikovani sertifikat, biće verifikovana upotreba liste i odgovarajućih informacija Registra kvalifikovanih Pružaoca usluga od poverenja.

Značajni datumi su:

- vreme izdavanja sertifikata za potpisivanje i
- vreme potpisivanja definisano u 0.

Prepoznata sertifikaciona tela izabranog pouzdanog servisa (za sertifikat i datume) se proveravaju u slučaju da postoje. Ako se ne pronađe izabrana pouzdana usluga, sertifikat za potpisivanje ili pečat se smatra nekvalifikovanim.

Definisanje da li se privatni ključ nalazi u uređaju za kreiranje kvalifikovanog potpisa

Da bi se proverilo da li je privatni ključ zaštićen na uređaju za kreiranje kvalifikovanog potpisa, biće verifikovano prisustvo iskaza uređaja za bezbedno kreiranje potpisa ili uređaja za kreiranje kvalifikovanog potpisa u sertifikatu.

Značajni datumi su:

- vreme izdavanja sertifikata za potpisivanje i
- vreme potpisivanja definisano u 0.

Uhvaćeni kvalifikatori izabranog pouzdanog servisa (za sertifikat i datume) se proveravaju za bezbedne uređaje kreiranja potpisa naredbu ili kvalifikovani uređaj za kreiranja potpisa u

slučaju da postoje. Ako nije pronađena nijedna odabrana pouzdana usluga, privatni ključ se smatra da nije kvalifikovani uređaj za kreiranje potpisa..

Definisanje vrste potpisa/pečata

Tip potpisa/pečata će biti određen na osnovu prisustva kombinacije izjava kvalifikovanog sertifikata i bezbednog uređaja za kreiranje potpisa ili uređaja za kreiranje kvalifikovanog potpisa u sertifikatu. Datumi od značaja su:

• vreme izdavanja sertifikata za potpisivanje i

• vreme potpisivanja definisano u 0.

Uhvaćeni kvalifikatori izabrane pouzdane usluge (za sertifikat i datume) se proveravaju u slučaju da postoje za izjave proširenja informacija o usluzi koje ukazuju na kvalifikovani sertifikat. Ako nije pronađena nijedna odabrana pouzdana usluga, vraća se tip definisan u sertifikatu.

Definisanje konzistentnosti tipa između sertifikata i liste poverenja

U slučaju da pouzdana usluga nema izjave o proširenju informacija o usluzi koje ukazuju na QC, proverava se prisustvo ekstenzija „Dodatne informacije o usluzi“ koje treba da bude u skladu sa definisanim tipom u sertifikatu.

3.2. Ulazna i izlazna ograničenja za procedure kreiranja, povećanja i validacije potpisa

3.2.1. Ulazna ograničenja koja će se koristiti prilikom generisanja, povećanja i/ili validacije potpisa u kontekstu identifikovane politike potpisa

Vreme validacije

Kao što je objašnjeno u odeljku 0, aplikacija za funkcionalnost može da obezbedi vreme validacije u zahtevu za validaciju potpisa. Ovo se može uraditi korišćenjem svojstva „verifyDate“ zahteva.

Proces validacije

Aplikacija za funkcionalnost takođe može navesti proces validacije koji treba da obavi aplikacija za proveru valjanosti potpisa tako što će obezbediti vrednost za svojstvo „verifyLevel“ zahteva.

Moguće vrednosti su:

- BASIC_SIGNATURES: odgovara ETSI TS 119 102-1 klauzula 5.3
- LONG_TERM_DATA: odgovara ETSI TS 119 102-1 klauzula 5.5
- ARCHIVAL_DATA (default): odgovara ETSI TS 119 102-1 klauzula 5.6.3.

3.2.3. Izlazna ograničenja koja će se koristiti za generisanje / povećanje potpisa u kontekstu identifikovane politike potpisa

Neprimenljivo.

4 Tehničke mere bezbednosti

4.1 Sigurnosne garancije

Pružalac usluge validacije koristi pouzdane sisteme i proizvode zaštićene od modifikacija. Za pružanje svojih usluga koristi jedinstven IT sistem koji se sastoji od pouzdanih, tehnički procenjenih i sertifikovanih bezbednosnih proizvoda.

Pružalac usluge validacije koristi pouzdane sisteme i proizvode koji su zaštićeni od neovlašćenih modifikacija.

Ako Pružalac usluge validacije koristi uslugu od poverenja treće strane, on će proveriti da li je ta treća strana u skladu sa svim neophodnim zahtevima.

Pružalac usluge validacije kreira ključeve za potpisivanje koji se koriste u potvrdama, ključeve koji se koriste za šifrovanje/dešifrovanje objekata validacije i infrastrukturnih i sistemskih kontrolnih ključeva u kriptografskom hardverskom uređaju. Pružalac usluge validacije povremeno zamenjuje ove ključeve. Pružalac usluge validacije prati razvoj tehnologije i ukoliko otkrije da ključ više nije bezbedan ili da algoritam više nije upotrebljiv prema odluci Ministarstva trgovine, turizma i telekomunikacija Republike Srbije, odmah zamenjuje pogođeni ključ ili ključevi.

4.2 Mere predostrožnosti za računarsku bezbednost

Pružalac usluga validacije koristi pouzdane IT sisteme i rešenja, tehnologije i razvija redundantni sistem. Dve instance rade za sve kritične komponente sistema pružaoca usluga, a u slučaju kvara bilo koje od tih jedinica, druga jedinica preuzima operaciju.

IT sistem Pružaoca usluge validacije je zaštićen višestepenim sistemom zaštitnog zida. Svaki zaštitni zid ima dve kopije, u slučaju kvara jedinice druga instanca iste jedinice preuzima njenu funkciju koristeći klaster.

4.3 Tehničke mere predostrožnosti vezane za životni ciklus

Da bi se ispunio visok nivo bezbednosnih zahteva u svim projektima razvoja sistema Pružaoca usluge validacije, povišeni zahtevi će se uzeti u obzir u celokupnom procesu razvoja (čak iu fazi planiranja i definisanja zahteva).

Proizvodi koji se koriste za pružanje usluga primenjuju se uzimajući u obzir bezbednosna pitanja vezana za životni ciklus.

4.4 Redovna sertifikacija

Pružalac usluge validacije je obavezan da stavi vremenski žig izdat od kvalifikovanog pružaoca ili da stavi vremenski žig na materijal za dugoročnu validaciju u sledećim slučajevima:

- ukoliko Ministarstvo trgovine, turizma i telekomunikacije donese takvu odluku;
- nakon obaveznog dostavljanja obaveštenja Ministarstvu trgovine, turizma i telekomunikacija o pokretanju postupka raspuštanja ili izricanju likvidacije Pružaoca usluge validacije.

4.5 Kontinuirano praćenje tehnilogije

Pružalac usluge validacije će kontinuirano pratiti razvoj tehnologije u vezi sa elektronskim potpisom i kriptografijom. Ukoliko Pružalac usluge validacije sazna da kriptografski algoritam sa datim parametrom koji je prihvaćen rešenjem Ministarstva trgovine, turizma i telekomunikacija Republike Srbije više nije bezbedan, o tome će obavestiti Ministarstvo trgovine, turizma i telekomunikacija. i zahtevati reviziju odluke u vezi sa kriptografskim algoritmima.

Pružalac usluge validacije može u bilo kom trenutku da odluči da promeni korišćene skupove kriptografskih algoritama i njihove parametre u slučaju da je algoritam i parametar prihvaćen rešenjem Ministarstva trgovine, turizma i telekomunikacija.

4.6 Prihvatanje Pružaoca sertifikata i vremenskog žigosanja

Pružalac usluga validacije može da navede pod kojim uslovima prihvata sertifikate datog sertifikacionog tela i koje autoritete za sertifikaciju prihvata, zajedno sa kriterijumima da autoriteti za sertifikaciju budu uključeni na ovu listu ili da budu isključeni iz nje u okviru dugoročna usluga validacije.

4.7 Dostupnost određenih elemenata usluge validacije

Godišnja dostupnost sledećih elemenata elektronske dugoročne usluge validacije je 99,7%, a povremeni prekidi usluge ne smeju biti duži od 1 dana:

- Usluga validacije

Pružalac usluge validacije ima pravo da suspenduje uslugu validacije.

5 Kontrole objekata, upravljanje i rada

Pružalac usluge validacije će primeniti fizičke, proceduralne i mere bezbednosti osoblja koje su u skladu sa priznatim standardima, zajedno sa administrativnim i upravnim procedurama koje ih primenjuju.

Pružalac usluge validacije vodi evidenciju o sistemskim jedinicama i resursima koji se odnose na pružanje usluge i vrši procenu rizika za njih. Koristiće zaštitne mere proporcionalne rizicima u vezi sa pojedinačnim elementima.
Pružalac usluge provere će pratiti zahteve za kapacitetom i obezbediće da su adekvatna procesorska snaga i skladištenje dostupni za pružanje usluge.

5.1 Fizičke kontrole

Pružalac usluge provere će se pobrinuti da fizički pristup kritičnim uslugama bude kontrolisan i da će fizički rizik imovine u vezi sa kritičnim uslugama držati na minimumu. Svrha fizičkih mera predostrožnosti je da spreči nelegitiman pristup, oštećenje i neovlašćeni pristup informacijama i fizičkim zonama Pružaoca usluge validacije.

Usluge koje obrađuju kritične i osetljive informacije biće implementirane na bezbednim lokacijama. Obezbeđena zaštita biće proporcionalna identifikovanim pretnjama analize rizika koju je izvršio Pružalac usluge validacije.

5.1.1 Lokacija i izgradnja

IT sistem Pružaoca usluga validacije će se nalaziti i funkcionisati u okviru propisno obezbeđenog Data centra sa fizičkom i logičkom zaštitom koja sprečava nelegitimne pristup.
Odbrambena rešenja – na primer zaštita, sigurnosne brave, sistemi za detekciju upada, sistem video nadzora, sistem kontrole pristupa – primenjivaće se tokom lociranja i uspostavljanja Data centara koji su međusobno izgrađeni i međusobno zavisni i zajedno pružaju moćan sistem zaštite IT sistema koji učestvuju u pružanju usluga, kao i za validaciju poverljivih podataka koje čuva pružalac.

5.1.2 Fizički pristup

Pružalac usluge validacije će zaštititi uređaje i opremu koji učestvuju u pružanju usluge od neovlašćenog fizičkog pristupa kako bi sprečio neovlašćeno korišćenje uređaja.

Pružalac usluga validacije će osigurati da:

- Svaki ulazak u Data centar ude registrovan;

- ulazak u Data centar može se desiti samo nakon istovremene identifikacije dva ovlašćena člana osoblja sa poverenim ulogama – a najmanje jedan od članova osoblja treba da bude administrator sistema;

- lica bez nezavisnog ovlašćenja mogu boraviti u Data centru samo u opravdanim slučajevima, potrebno vreme iu pratnji osoblja sa odgovarajućim pravima;

- dnevnici unosa će se arhivirati kontinuirano i evaluirati sedmično.

Aktivacioni podaci (lozinke, PIN kodovi) uređaja neće se čuvati otvoreno čak ni u Data centru.

U prisustvu neovlašćenih lica:

- mediji sa podacima koji sadrže osetljive informacije treba da budu fizički van domašaja;

- prijavljeni terminali ne smeju ostati bez nadzora;

ne bi trebalo da se sprovodi radni proces tokom kojeg se mogu otkriti poverljive informacije.

Prilikom napuštanja računarske sobe administrator će proveriti da:

- svaka oprema Data centra je u adekvatno bezbednom radnom stanju;

- nijedan terminal nije ostao prijavljen;

- fizički uređaju za skladištenje su pravilno zaključani;

- sistemi, uređaji koji pružaju fizičku zaštitu rade ispravno;

- alarmni sistem je aktiviran.

Trebalo bi da budu imenovani odgovorni ljudi koji će vršiti redovne procene fizičke bezbednosti. Rezultati ispitivanja se upisuju u odgovarajuće evidencije.

5.1.3 Napajanje i klimatizacija

Pružalac usluge validacije će primeniti jedinicu za neprekidno napajanje u Data centru koja:

- ima adekvatan kapacitet da obezbedi napajanje za IT i sisteme pomoćnih objekata Data centra;

- štiti IT opremu od fluktuacija napona u spoljnoj mreži, nestanka struje, naponskih skokova i drugo,

- u slučaju dugotrajnog nestanka struje ima sopstvenu opremu za proizvodnju električne energije, koja je – omogućavanjem dopunjavanja – u stanju da obezbedi neophodnu energiju za bilo koji vremenski period.

Vazduh iz spoljašnje sredine ne sme da ulazi direktno u Data centar. Vazduh u Data centru čistoća će biti obezbeđena adekvatnim sistemom filtera za otkrivanje raznih zagađivača iz vazduh (prašina, zagađivači i korozivni materijali, toksične ili zapaljive materije). Ventilacija sistem treba da obezbedi neophodnu količinu svežeg vazduha sa odgovarajućom filtracijom za bezbednost uslove rada operatera.
Vlažnost treba smanjiti na nivo koji zahtevaju IT sistemi.
Sistemi za hlađenje sa odgovarajućim performansama treba da se koriste da bi se obezbedio neophodan rad temperature, kako bi se sprečilo pregrevanje IT uređaja.

5.1.4 Izloženost vodi

Data centar Pružaoca usluge validacije biće adekvatno zaštićen od prodora vode i poplava.

5.1.5 Prevencija i zaštita od požara

Detektori dima i požara će biti instalirani u Data Centru Pružaoca usluge validacije koji automatski upozoravaju vatrogasnu jedinicu. Ručne aparate za gašenje požara odgovarajuće vrste i količine u skladu sa relevantnim propisima treba postaviti na vidno mesto u svakoj prostoriji.
U Data centru se primenjuju automatski aparati za gašenje požara.

5.1.6 Skladištenje medija

Pružalac usluge validacije će zaštititi svoje medijske skladišta od neovlašćenog pristupa i slučajnog oštećenja. Svi revizijski i arhivski podaci kreiraju se u duplikatu. Dve kopije treba da se čuvaju odvojeno jedna od druge fizički, na lokacijama na bezbednoj udaljenosti jedna od druge.
Skladišteni mediji moraju biti zaštićeni od štetnih uticaja okoline kao što su niske ili visoke temperature, prljavština, vlaga, sunčeva svetlost, jaka magnetna polja, jako zračenje.

5.1.7 Odlaganje otpada

Pružalac usluge validacije će se pobrinuti za uništavanje svojih uređaja, a medijske memorije postaju suvišne u skladu sa ekološkim propisima. Takvi uređaji i skladišta medija biće trajno obrisani ili neupotrebljivi u skladu sa opšteprihvaćenim metodama pod ličnim nadzorom zaposlenih Pružaoca usluge validacije.

5.1.8 Rezervna kopija van lokacije

Pružalac usluge validacije će svake nedelje kreirati rezervnu kopiju iz koje bi se cela usluga mogla vratiti u slučaju fatalne greške.
Rezervne kopije – barem uključujući poslednju potpunu rezervnu kopiju – biće uskladištene na spoljnoj lokaciji čija je fizička i operativna zaštita identična primarnoj lokaciji. Bezbedan prenos podataka sa primarnih na rezervne lokacije će biti rešen.
Na osnovu nasumično odabranih rezervnih podataka, test restauracije će se raditi najmanje jednom godišnje. Glavne okolnosti i rezultati testa restauracije biće zabeleženi u izveštaju revizije.

5.2 Proceduralne kontrole

Pružalac usluge validacije će se pobrinuti da njegovi sistemi rade bezbedno, u skladu sa pravilima i sa minimalnim rizikom od kvarova.
Proceduralne mere predostrožnosti imaju za cilj da dopune i u isto vreme pojačaju delotvornost fizičkih zaštitnih mera, zajedno sa onima koje se primenjuju na osoblje, putem imenovanje i izolovanje pouzdanih uloga, dokumentovanje odgovornosti različitih uloga, kao i preciziranje broja zaposlenih i uloga isključivanja neophodnih za različite zadatke, štaviše identifikacija i autentifikacija koja se očekuje u različitim ulogama.

Interni sistem upravljanja Pružaoca usluga validacije osigurava da je njegov rad u skladu sa zakonskim, kao i internim propisima. U njegovom sistemu će za svaku datu sistemsku jedinicu i proces jasno biti određena odgovorna osoba.

Pojedinci odgovorni za dati element sistema ili proces biće nedvosmisleno dodeljeni svakom elementu sistema i svakom procesu u njegovom sistemu. Zadaci koji se odnose na razvoj i operacije oštro su razdvojeni u sistemu Pružaoca usluga validacije. Revizijska aktivnost nezavisnog revizora sistema i internog revizora pružaoca usluga validacije obezbeđuje odgovarajući rad sistema.

5.2.1 Povereničke uloge

Pružalac usluge validacije će kreirati pouzdane uloge za obavljanje svojih zadataka. Prava i funkcije će biti podeljene među različitim pouzdanim ulogama na način da jedan korisnik sam ne može da zaobiđe mere bezbednosti.
Povereničke uloge koje treba primeniti:

- Menadžer implementacije za IT sistem provajdera;
- službenik obezbeđenja: pojedinac sa opštom odgovornošću za bezbednost službe;
- sistem administrator: pojedinac koji obavlja instalaciju, konfiguraciju IT sistema i održavanje;
- operater: pojedinac koji obavlja kontinuirani rad IT sistema, pravljenje rezervnih kopija i vraćanje u prethodno stanje;
- nezavisni revizor sistema: lice koje vrši reviziju evidentiranog, kao i arhiviranog skupa podataka provajdera, odgovorno za proveru sprovođenja kontrolnih mera koje provajder sprovodi u interesu poslovanja u skladu sa propisima, štaviše za kontinuiranu reviziju i praćenje postojećih procedure.
- službenik za validaciju: moguće je dešifrovati objekat za validaciju uz saradnju dva dugoročna službenika za validaciju. Službenici za dugoročnu validaciju odgovorni su za bezbedno upravljanje dešifrovanim objektom za validaciju i za njegovo uništenje.
- službenik odgovoran za izdavanje dugoročne izjave o validaciji: njegova dužnost je izdavanje i sertifikacija dugoročnih izjava o validaciji.

Za obezbeđivanje pouzdanih uloga, menadžer odgovoran za bezbednost Pružaoca usluga validacije će formalno imenovati zaposlene Pružaoca usluga validacije.
Samo one osobe mogu imati ulogu od poverenja koje su u radnom odnosu sa Pružaocem usluga validacije. Povereničke uloge neće se obavljati u kontekstu ugovora o proviziji.
Vodiće se ažurna evidencija o poverenim ulogama iu slučaju bilo kakve promene, Ministarstvo trgovine, turizma i telekomunikacija biće obavešteno bez odlaganja.

5.2.2 Broj potrebnih osoba po zadatku

Bezbednosnim i operativnim propisima Pružaoca usluge validacije treba da se definiše da se sledeći poslovi mogu obavljati samo u zaštićenom okruženju, uz istovremeno prisustvo dva zaposlena koja imaju povereničke uloge:

- generisanje sopstvenog para ključeva usluge Pružaoca usluge validacije;
- rezervnu kopiju privatnog ključa Pružaoca;

- aktiviranje privatnog ključa Pružaoca;

- uništavanje privatnog ključa Pružaoca.

Najmanje jedno od lica koja obavljaju gore navedene procedure mora biti administrator sistema, a drugo lice ne može biti nezavisni revizor sistema.
Saradnja dva službenika za proveru valjanosti je neophodna za dešifrovanje šifrovanog objekta provere koji se čuva u arhivi. Službenici za validaciju su odgovorni za bezbedno upravljanje dešifrovanim objektom validacije i za njegovo uništenje.

U toku sprovođenja navedenih radnji u prostoriji se ne smeju nalaziti neovlašćena lica.

5.2.3 Identifikacija i autentifikacija za svaku ulogu

Korisnici koji upravljaju IT sistemom Pružaoca usluge validacije moraju imati jedinstvene identifikacione podatke, koji omogućavaju sigurnu identifikaciju i autentifikaciju korisnika.
Korisnici mogu pristupiti IT sistemima koji su kritični sa aspekta pružanja usluge sertifikacije tek nakon identifikacije i autentifikacije.
Podaci za identifikaciju i autentifikaciju će se bez odlaganja opozvati u slučaju prestanka prava korisnika.

5.2.4 Uloge koje zahtevaju razdvajanje dužnosti

Zaposleni kod Pružaoca usluge validacije mogu istovremeno imati više pouzdanih uloga, ali je Pružalac usluge validacije obavezan da obezbedi da:

- službenik za bezbednost i službenik za registraciju neće imati ulogu nezavisnog revizora sistema;

- administrator sistema neće držati službenika za bezbednost i nezavisni sistem uloga revizora;

- menadžer sa opštom odgovornošću za IT sistem neće imati službenika za bezbednost i nezavisnog revizora sistema.

5.3 Kontrola osoblja

Pružalac usluge validacije će se pobrinuti da njegova kadrovska politika i njegove prakse primenljive na zapošljavanje članova osoblja intenziviraju i podržavaju pouzdanost rada Pružaoca usluge validacije.
Cilj mera predostrožnosti koje se primenjuju na osoblje je smanjenje rizika od ljudskih grešaka, krađe, prevare i slučajeva zloupotrebe.

Pružalac usluge validacije će se pozabaviti bezbednošću osoblja već tokom faze zapošljavanja, uključujući zaključivanje ugovora, kao i njihovu validaciju kada su zaposleni. U slučaju svih uloga od poverenja, kandidati će imati važeće uverenje o neosuđivanosti u vreme podnošenja prijave. Svaki zaposleni u ulozi od poverenja i spoljne strane koje stupe u kontakt sa uslugama Pružaocem usluge validacije potpisaće ugovor o neotkrivanju podataka.
Istovremeno, Pružalac usluge validacije će svojim zaposlenima obezbediti sticanje i dalje razvijanje zajedničkog, opšteg znanja i specijalizovanih stručnih znanja neophodnih za obavljanje različitih poslova.

5.3.1 Zahtevi za kvalifikacije, iskustvo i odobrenje

Svaki zaposleni kod Pružaoca usluga validacije mora imati neophodno obrazovanje, praksu i profesionalno iskustvo za pružanje svog delokruga.

Pouzdane uloge kod Pružaoca usluga validacije mogu obavljati samo osobe koje nemaju spoljni uticaj i koje poseduju neophodnu stručnost koju je proveravao Pružalac usluge validacije. Svo osoblje u pouzdanim ulogama neće biti u sukobu interesa koji bi mogao ugroziti nepristrasnost operacija Pružaoca usluge validacije.

Menadžer sa ukupnom odgovornošću za IT sistem može biti samo osoba koja ima:

- specijalizovana diploma (matematika, informacione tehnologije) višu ili fakultetsku diplomu ili višu/visoku diplomu stečenu na inženjerskom odseku iz tehničke oblasti nauke);

- najmanje tri godine stručnog iskustva u profesionalnom radnom iskustvu u oblasti informacione bezbednosti.

5.3.2 Procedure provere pozadine

Pružalac usluga validacije će angažovati samo zaposlene za pouzdane ili vodeće uloge, koji

- imaju čist dosije i protiv njih nije u toku nikakav postupak koji može uticati na nekažnjivost.

- ne podležu profesionalnim diskvalifikacijama koje zabranjuju korišćenje usluga u vezi sa elektronskim potpisom.

Da li će u vreme imenovanja nosilac vodeće uloge, zaposlenik kod Pružaoca usluga validacije sa izjavom, službenik nosioca uloge od poverenja sa sertifikatom o dobrom ponašanju starom manje od 6 meseci, opravdati čist krivični dosije.

Pružalac usluge validacije verodostojnosti relevantnih informacija navedenih u biografiji kandidata tokom procesa zapošljavanja, kao što su prethodno zaposlenje, profesionalne reference i najrelevantnije obrazovne kvalifikacije.

5.3.3 Zahtevi za obuku

Pružalac usluge validacije će obučiti novoprimljene zaposlene, tokom koje stiču

- osnovno PKI znanje;
- specifičnosti i način rukovanja IT sistemom Pružaoca usluge validacije;
- neophodna posebna znanja za obavljanje njihovog delokruga;
- procesi i procedure definisane u javnom i internim propisima Pružaoca usluge validacije;
- pravne posledice pojedinačnih aktivnosti;
- važeći propisi o IT bezbednosti u meri u kojoj je to neophodno za specifičan obim aktivnosti;
- pravila o zaštiti podataka.

Samo zaposleni koji su prošli obuku dobijaju pristup proizvodnom IT sistemu Pružaoca usluge validacije.

5.3.4 Učestalost i uslovi prekvalifikacije

Pružalac usluge validacije će obezbediti da zaposleni poseduju neophodna znanja u kontinuitetu, pa će se po potrebi održati dodatna ili ponavljajuća obuka.
Dalja obuka će se održati ako dođe do promene u procesima ili IT sistemu Pružaoca usluge validacije.
Obuka mora biti adekvatno dokumentovana, iz čega se može jasno odrediti nastavni plan i obim zaposlenih učesnika.

5.3.5 Učestalost i redosled rotacije poslova

Bez odredbe.

5.3.6 Sankcije za nedozvoljene radnje

Pružalac usluge validacije će ugovorom o radu regulisati mogućnosti krivičnog gonjenja zaposlenih u slučaju propusta, grešaka, slučajnog ili namernog oštećenja.
Ukoliko zaposleni – zbog nemara ili namerno – prekrši svoje obaveze, protiv njega može biti izrečena sankcija od strane Pružaoca usluge validacije, koje on odredi s obzirom na prekršaj

i posledice. Sankcije mogu uključivati disciplinski postupak, razrešenje, opoziv imenovanja, krivičnu odgovornost.

5.3.7 Zahtevi nezavisnog izvođača

Na radnike zaposlene u ugovornom odnosu primenjuju se ista pravila kao i na zaposlene.

Nosilac uloge od poverenja biće u radnom odnosu sa Pružaocem usluga validacije.

5.3.8 Dokumentacija dostavljena osoblju

Pružalac usluga provere će kontinuirano obezbeđivati zaposlenima dostupnost aktuelne dokumentacije i propisa neophodnih za obavljanje njihovih uloga.

5.4 Procedure evidentiranja revizije

Da bi održao bezbedno IT okruženje, Pružalac usluga validacije će implementirati i upravljati evidentiranjem događaja i kontrolnim sistemom koji pokriva njegov kompletan IT sistem.

5.4.1 Vrste snimljenih događaja

Pružalac usluge validacije će evidentirati svaki događaj vezan za bezbednost koji može da pruži informacije o događajima, promenama koje se dešavaju u IT sistemu ili njegovom fizičkom okruženju u skladu sa opšteprihvaćenom praksom bezbednosti informacija. U slučaju svakog unosa u dnevnik, čuvaju se sledeći podaci:

- vreme događaja;
- vrsta događaja;
- identifikacija korisnika ili sistema koji je pokrenuo događaj;
- uspeh ili neuspeh revidovanog događaja.

Revizorski zapisi se ne smeju menjati ili brisati.
Svi bitni dnevnici događaja biće dostupni nezavisnim revizorima sistema, koji ispituju usklađenost rada Pružaoca usluge validacije.

Sledeći događaji se moraju evidentirati najmanje:

- UNUTRAŠNJI SAT
  - sinhronizaciju unutrašnjeg sata sa UTC vremenom, uključujući i operativne ponovne kalibracije;
  - gubitak sinhronizacije;
- VALIDACIJA
  - informacije koje se odnose na dostupnost podataka, integritet validiranih potpisa, autentičnost, održavanje čitljivosti i brisanje informacija;
  - informacije vezane za preuzimanje dokaza o validaciji, ispunjenje zahteva za izjavu i predaju arhive drugom provajderu;
- LOGOVANJE:
  - gašenje, ponovno pokretanje sistema za logovanje ili neke njegove komponente;
  - izmenu bilo kog parametra podešavanja logovanja, na primer učestalosti, praga upozorenja i događaja koji treba ispitati;
  - izmenu ili brisanje sačuvanih podataka logovanja;
  - aktivnosti koje se obavljaju zbog kvara sistema logovanja.

- SISTEMSKA PRIJAVA:
  - uspešne prijave, neuspešni pokušaji prijavljivanja za pouzdane uloge;
  - u slučaju autentifikacije zasnovane na lozinki:
    - promena broja dozvoljenih neuspešnih pokušaja;
    - dostizanje granice dozvoljenog broja neuspešnih pokušaja prijavljivanja u slučaju prijavljivanja korisnika;
    - blokiran ponovni prijem korisnika zbog neuspešnih pokušaja prijave;
  - promena tehnike autentifikacije (na primer sa lozinke na baziranu na PKI-ju).
- UPRAVLJANJE KLJUČA:
  - svi događaji za ceo životni ciklus servisnih ključeva (generisanje ključeva, čuvanje, učitavanje, uništavanje itd.);
- TOKOVI PODATAKA:
  - bilo koju vrstu bezbednosno kritičnih podataka koji se ručno unose u sistem;
  - podaci relevantni za bezbednost, poruke koje sistem prima;
- Hardverski sigurnosni modul:
  - instaliranje hardverskog sigurnosnog modula;
  - uklanjanje hardverskog bezbednosnog modula;
  - odlaganje, uništavanje hardverskog bezbednosnog modula;
  - isporuka hardverskog sigurnosnog modula;
  - brisanje (resetovanje) hardverskog bezbednosnog modula;
  - učitavanje ključeva, sertifikata u hardverski sigurnosni modul.
- PROMENA KONFIGURACIJE:
  - hardver;
  - softver;

  - operativni sistem;
  - peč;
  - instaliranje, ažuriranje i uklanjanje softvera na sistemu sertifikata;

- FIZIČKI PRISTUP, BEZBEDNOST LOKACIJE:
  - ulazak i izlazak lica iz bezbednosne zone u kojoj se nalaze komponente sistema koje se koriste za pružanje usluge poverenja;
  - pristup sistemskoj komponenti koja se koristi za Pružanje usluge poverenja;
  - poznato ili sumnjivo kršenje fizičkog obezbeđenja;
  - saobraćaj zaštitnog zida ili rutera.

- OPERATIVNE ANOMALIJE:
  - pad sistema, kvar hardvera;
  - kvarovi u softveru;
  - greška u validaciji integriteta softvera;
  - netačne ili pogrešno adresirane poruke;
  - mrežni napadi, pokušaji napada;
  - kvar opreme;
  - kvarovi električne energije;
  - greška u neprekidnom napajanju;
  - suštinska greška u pristupu mrežnoj usluzi;
  - kršenje Izjave o praksi validacije;
  - brisanje sata operativnog sistema.

- OSTALI DOGAĐAJI:
  - imenovanje lica na bezbednosnu ulogu;
  - instalacija operativnog sistema;
  - instalacija PKI aplikacije;

- pokretanje sistema;
- pokušaj ulaska u PKI aplikaciju;
- izmena lozinke, pokušaj podešavanja;
- čuvanje unutrašnje baze podataka i vraćanje iz rezervne kopije;
- operacije sa datotekama (na primer kreiranje, preimenovanje, premeštanje);
- pristup bazi podataka.

5.4.2 Učestalost obrade dnevnika revizije

Pružalac usluge validacije će obezbediti redovnu procenu kreiranih dnevnika.
Kreirani dnevni log fajlovi će se proceniti sledećeg radnog dana ako je moguće, ali najkasnije u roku od 1 nedelje.

Procenu datoteka evidencije će izvršiti nezavisni revizor sistema sa odgovarajućom stručnošću, sistemskim privilegijama i imenovanjem.

Pružalac usluge validacije može da koristi automatizovane alate da pomogne u proceni elektronskih dnevnika. Obaveštenja dobijena od automatizovanih alata za praćenje biće obrađena i procenjena u roku od 24 sata.

Tokom ocenjivanja treba da se obezbedi autentičnost i integritet pregledanih dnevnika.

Tokom evaluacije, sistemski generisane poruke o grešci će biti analizirane.
Značajne promene u saobraćaju treba analizirati statističkim metodama. Činjenica revizije, rezultati revizije i mere preduzete u cilju otklanjanja svih utvrđenih nedostataka moraju biti propisno dokumentovani.

5.4.3 Period zadržavanja za evidenciju revizije

Pre brisanja iz onlajn sistema, evidencije će biti arhivirane i njihova bezbedna validacija će biti obezbeđena tokom perioda definisanog u odeljku 5.5.2.

5.4.4 Zaštita dnevnika revizije

Pružalac usluge validacije štiti kreirane evidencije sve dok je validnost dokaza validacije osigurana sledeća svojstva podataka evidencije:

- zaštita od neovlašćenog otkrivanja: samo ovlašćena lica – prvenstveno nezavisni revizori sistema – imaju pristup evidenciji;

- dostupnost: ovlašćenim licima će biti omogućen pristup evidenciji;

- integritet: biće sprečena svaka promena podataka, brisanje u fajlovima logovanje i promena redosleda unosa itd.

5.4.5 Procedure za pravljenje rezervnih kopija dnevnika revizije

Dnevni log fajlovi će se kreirati od kontinuirano generisanih unosa dnevnika tokom rada u svakom sistemu.
Dnevni log fajlovi će biti arhivirani u dva primerka nakon evaluacije i uskladišteni fizički odvojeno jedan od drugog, na odvojenim lokacijama u potrebnom vremenu. Tačan proces pravljenja rezervnih kopija biće definisan u Izjavi o praksi validacije.

5.4.6 Sistem prikupljanja revizije (interni naspram eksternog)

Pružalac usluge validacije specificira rad svojih procesa evidentiranja u svojoj Izjavi o praksi validacije.
Pružalac usluge validacije može da koristi automatske sisteme revizije i evidentiranja ako može da obezbedi da su aktivni u vreme pokretanja sistema i da rade neprekidno do isključivanja sistema.

Ako postoji bilo kakva anomalija u sistemima za automatsku reviziju i evidentiranje, rad Pružaoca usluge provere će biti suspendovan dok se incident ne reši.

5.4.7 Obaveštenje subjektu koji izaziva događaj

U slučaju otkrivenih grešaka, Pružalac usluge validacije po sopstvenom nahođenju može odlučiti da li će obavestiti osobu, ulogu, uređaj ili aplikaciju o grešci koja je do nje izazvala.

5.4.8 Procene ugroženosti

Procenu ugroženosti će svake godine sprovoditi Pružalac usluge validacije kako bi pomogao u otkrivanju potencijalnih unutrašnjih i eksternih pretnji, koje mogu dovesti do neovlašćenog pristupa.

Takođe će se mapirati verovatnoća nastanka događaja i očekivana šteta.
Redovno procenjuje sprovedene procese, mere bezbednosti, informacione sisteme, tako da su u stanju da pravilno izdrže otkrivene pretnje.

Nakon procene uočenih grešaka, ukoliko je potrebno, sistem odbrane će biti izmenjen kako bi se sprečile slične greške u budućnosti.

5.5 Kompromitovanje i oporavak od katastrofe

U slučaju havarije, Pružalac usluge validacije je dužan da preduzme sve neophodne mere kako bi minimizirao štetu nastalu usled nedostatka usluge i što pre obnovi usluge. Na osnovu procene incidenta koji se dogodio, preduzeće potrebne izmene, korektivne mere za sprečavanje budućeg nastanka incidenta.
Kada se problem reši, događaj će biti prijavljen Ministarstvu trgovine, turizma i telekomunikacija, kao nadzornom organu.

5.5.1 Procedure za rukovanje incidentima i kompromitovanjem

Pružalac usluge validacije ima plan kontinuiteta poslovanja.
Pružalac usluge validacije će uspostaviti i održavati potpuno funkcionalan rezervni sistem, koji je na bezbednoj udaljenosti od primarne lokacije, geografski lociran na drugom mestu i koji je nezavisno sposoban da pruži pun spektar usluga.
Pružalac usluge validacije će kontinuirano testirati rad rezervnog sistema i pregledaće svoje planove za kontinuitet poslovanja svake godine.
U slučaju katastrofe, dostupnost usluga će se vratiti što je pre moguće.

5.5.2 Računarski resursi, softver i/ili podaci su oštećeni

IT sistemi Pružaoca usluga validacije biće izgrađeni od pouzdanih hardverskih i softverskih komponenti. Kritične funkcije će se realizovati korišćenjem redundantnih elemenata sistema tako da u slučaju kvara stavke mogu dalje da rade.

Pružalac usluge validacije će napraviti punu dnevnu rezervnu kopiju svojih baza podataka i generisanih događaja evidencije.

Pružalac usluge validacije će praviti potpune rezervne kopije onoliko često koliko je potrebno da bi mogao da vrati punu uslugu u slučaju katastrofe.

Plan kontinuiteta poslovanja Pružaoca usluga validacije će uključiti tačne zahteve za zadatke koje treba izvršiti u slučaju kvara kritične komponente sistema.
Kada se problem reši i integritet povrati, Pružalac usluge validacije će ponovo pokrenuti svoje usluge što je pre moguće.

5.5.3 Mogućnosti kontinuiteta poslovanja nakon katastrofe

Zadaci koji se obavljaju u slučaju kvara usluge usled prirodne ili druge nepogode biće definisani planom kontinuiteta poslovanja Pružaoca usluga validacije.

U slučaju katastrofe, propisi stupaju na snagu, počeće kontrola štete i obnavljanje usluga. Lokacija sekundarnih usluga biće postavljena tako daleko od primarne lokacije da verovatna katastrofa ne može istovremeno stići na obe lokacije.
Pružalac usluge validacije je dužan da u slučaju katastrofe obavesti pogođene korisnike što je pre moguće.

Nakon obnavljanja usluga, Pružalac usluge validacije će vratiti svoje uređaje oštećene tokom katastrofe i prvobitni nivo bezbednosti usluge što je pre moguće.

5.6 Prestanak usluge validacije

Pružalac usluge validacije će se pridržavati zahteva propisanih u zakonodavstvu u slučaju prekida usluge.

Tokom raskida prioritetni zadaci su:

- Zavisne strane i Pretplatnici će biti blagovremeno obavešteni o planiranom prekidu;
- Pružalac usluge validacije će učiniti sve da obezbedi da najkasnije do prestanka usluge drugi pružalac preuzme evidenciju i obaveze usluge;
- nakon prestanka usluge, izvršiće se potpuna rezervna kopija i arhiviranje sistema;
- arhivirani podaci predaju se pružaocu koji preuzima usluge, odnosno Ministarstvo trgovine, turizma i telekomunikacija.

6 Tehničke bezbednosne kontrole

Pružalac usluga validacije će koristiti pouzdane sisteme i opremu zaštićenu od modifikacija za upravljanje kriptografskim ključevima i podacima za aktivaciju tokom celog životnog ciklusa. Potrebe za kapacitetima će se kontinuirano pratiti i procenjivati buduće potrebe za kapacitetom, kako bi se obezbedila neophodna dostupnost potreba za preradom i skladištenjem.

6.1 Zaštita privatnog ključa i inženjerske kontrole kriptografskog modula

Pružalac usluge validacije će obezbediti bezbedno upravljanje privatnim ključevima koje poseduje i sprečiće otkrivanje, kopiranje, brisanje, modifikovanje i neovlašćeno korišćenje privatnog ključa. Pružalac usluge validacije može čuvati privatne ključeve samo sve dok pružanje usluge definitivno zahteva.

Tokom upravljanja hardverskim sigurnosnim modulima čuvaju se potpisujući privatni ključevi hardverski sigurnosni moduli koji nisu u funkciji biće obrisani tako da je praktično nemoguće vratiti ključeve.

6.1.1 Standardi i kontrole kriptografskog modula

Sistemi Pružaoca usluga validacije će čuvati privatne ključeve u takvim bezbednim hardverskim uređajima koji su u skladu sa sledećim:

- zahtevima ISO/IEC 19790 [4], ili
- zahtevima FIPS 140-2 [5] nivoa 3 ili više, ili
- zahtevima FIPS 140-3 [6] nivoa 3 ili više, ili
- zahtevima CEN 419 221-5 [7], ili
- oni su tako pouzdani sistemi koji se procenjuju na nivou garancije 4 ili više prema ISO/IEC 15408 [8] ili ekvivalentnom sistemu bezbednosnih kriterijuma. Procena će se zasnivati ili na odgovarajućem planu sistema bezbednosti koji ispunjava zahteve ovog dokumenta, ili na aproprijacijama za bezbednost.

Ključevi Pružaoca mogu da se čuvaju samo u šifrovanim oblicima izvan hardverskog bezbednosnog modula. Za kodiranje će se koristiti samo oni algoritmi i parametri ključa za koje se očekuje da će moći da izdrže kriptografske napade tokom čitavog životnog veka ključeva.

Privatni ključevi Pružaoca će se čuvati na fizički bezbednoj lokaciji čak iu šifrovanom obliku, gde su dostupni samo ovlašćenim osobama.
U slučaju slabljenja kriptografskih algoritama i parametara ključa, kodirani ključevi se uništavaju ili se ponovo kodiraju korišćenjem algoritma i parametara ključa koji obezbeđuju veću zaštitu.

6.1.2 Privatni ključ (N od M) Kontrola više osoba

Pružalac usluge validacije će osigurati da istovremeno prisustvo najmanje dvoje; zaposleni nosioci uloge od poverenja su potrebni za kritične operacije koje se obavljaju sa privatnim ključevima Pružaoca.

6.1.3 Deponovanje privatnog ključa

Pružalac usluge provere može da deponuje privatne ključeve sopstvenog provajdera samo u šifrovanom obliku.

6.1.4 Rezervna kopija privatnog ključa

Pružalac usluge provere će napraviti sigurnosne kopije privatnih ključeva svog provajdera, a najmanje jedna kopija njih će biti uskladištena na drugom mestu od lokacije pružaoca usluge. Pravljenje rezervnih kopija se može vršiti samo u zaštićenom okruženju, uz istovremeno prisustvo najmanje dve osobe koje imaju poverene uloge, uz isključenje drugih ljudi.
Najmanje isti strogi bezbednosni standardi biće primenjeni na upravljanje i validaciju rezervnih kopija kao i za rad proizvodnog sistema.

6.1.5 Arhiviranje privatnog ključa

Pružalac usluge validacije neće arhivirati svoje privatne ključeve.

6.1.6 Prenos privatnog ključa u ili iz kriptografskog modula

Svi privatni ključevi provajdera Pružaoca usluge validacije biće kreirani u kriptografskom modulu koji ispunjava zahteve.

Privatni ključevi neće postojati u otvorenom obliku izvan hardverskog bezbednosnog modula.

Pružalac usluge validacije može samo da eksportuje privatni ključ iz hardverskog bezbednosnog modula u svrhu pravljenja bezbedne kopije.

Prenos privatnog ključa između hardverskih sigurnosnih modula je dozvoljen samo u obliku bezbedne kopije.

6.1.7 Skladištenje privatnog ključa na kriptografskom modulu

Pružalac usluge validacije će čuvati privatne ključeve koji se koriste za pružanje usluge u skladu sa ovim smernicama sertifikata u hardverskom bezbednosnom modulu.
Ne postoji ograničavajući termin koji se primenjuje za obrazac za skladištenje u hardverskom bezbednosnom modulu.

6.1.8 Način aktiviranja privatnog ključa

Privatni ključevi Pružaoca usluge validacije će biti aktivirani u skladu sa procedurama i zahtevima definisanim u korisničkom vodiču za korišćeni kriptografski modul i sertifikacionim dokumentima.

6.1.9 Metoda deaktiviranja privatnog ključa

Privatni ključevi Pružaoca usluge validacije će biti deaktivirani u skladu sa procedurama, zahtevima definisanim u korisničkom vodiču za korišćeni hardverski bezbednosni modul i sertifikacionim dokumentima.

6.1.10 Metoda uništavanja privatnog ključa

Odbačeni, istekli ili kompromitovani privatni ključevi Pružaoca usluge validacije biće uništeni na način koji onemogućava dalju upotrebu privatnih ključeva.
Privatni ključevi Pružaoca biće uništeni u skladu sa procedurama, zahtevima definisanim u korisničkom vodiču i u sertifikacionim dokumentima korišćenog hardverskog bezbednosnog modula, u istovremenom prisustvu dva zaposlena kod Pružaoca usluge validacije (administratora infrastrukture i službenika bezbednosti) sa isključenjem drugih lica.

Svaka rezervna kopija privatnog ključa biće uništena na dokumentovan način na način da njeno vraćanje i korišćenje postane nemoguće.

6.1.11 Ocena kriptografskog modula

U skladu sa zahtevima odeljka 6.1.1, svaki privatni ključ Pružaoca usluge validacije će biti uskladišten u kriptografskom modulu koji

- ima sertifikat prema ISO/IEC 19790 [4], ili
- ima sertifikat prema FIPS 140-2 nivo 3 [5], ili
- ima sertifikat prema FIPS 140-3 nivo 3 [6], ili

- ima sertifikat zasnovan na zajedničkim kriterijumima najmanje EAL-4 nivoa [9] koji potvrđuje usklađenost sa zahtevima CEN 419 221-5 [7], ili

- ima sertifikat izdat u tu svrhu od nezavisnog sertifikacionog tela kvalifikovanog za procenu proizvoda elektronskog potpisa, registrovanog od strane Ministarstva trgovine, turizma i telekomunikacija, ili u državi članici Evropske unije.

6.2 Podaci o aktivaciji

6.2.1 Generisanje i instalacija aktivacionih podataka

Privatni ključevi Pružaoca usluge validacije će biti zaštićeni u skladu sa procedurama, zahtevima definisanim u korisničkom vodiču za korišćeni hardverski bezbednosni modul i sertifikacionim dokumentima.
U slučaju korišćenja podataka za aktiviranje zasnovane na lozinki, lozinke moraju biti dovoljno složene da bi se obezbedio potreban nivo zaštite.

6.2.2 Zaštita podataka aktivacije

Uređaje, podatke za aktivaciju neophodne za aktivaciju privatnog ključa bezbedno će čuvati zaposleni Pružaoca usluge validacije, lozinke se mogu čuvati samo kodirane.

6.2.3 Drugi aspekti aktivacionih podataka

Bez odredbe.

6.3 Kontrole kompjuterske bezbednosti

6.3.1 Specifični tehnički zahtevi za bezbednost računara

Tokom konfiguracije i rada IT sistema Pružaoca usluga validacije obezbediće se usaglašenost sa sledećim zahtevima:

- dentitet korisnika se verifikuje pre odobravanja pristupa sistemu ili aplikaciji;

- uloge se dodeljuju korisnicima i mora se obezbediti da svi korisnici imaju samo dozvole prikladan za svoje uloge;

- zapis u dnevniku se kreira za svaku transakciju, a unosi se arhiviraju;

- za bezbednosno kritične procese obezbeđuje se da su interni mrežni domeni Pružaoca usluge validacije dovoljno zaštićeni od neovlašćenog pristupa;

- primenjuju se odgovarajuće procedure da bi se obezbedio oporavak usluge nakon gubitka ključa ili otkaza sistema.

6.3.2 Ocena računarske bezbednosti

Da bi obezbedio IT bezbednost i kvalitet usluge, Pružalac usluga validacije će implementirati sistem kontrole po međunarodno prihvaćenim metodologijama, a adekvatnost istih će biti potvrđena sertifikatom izdatim od nezavisnog sertifikacionog tela..

6.4 Tehničke kontrole životnog ciklusa

6.4.1 Kontrole razvoja sistema

Pružalac usluge validacije će koristiti samo aplikacije i uređaje u svom proizvodnom IT sistemu koji:

- komercijalni softver u kutiji, dizajniran i razvijen prema dokumentovanoj metodologiji dizajna, ili;

- prilagođena hardverska i softverska rešenja razvijena od strane samog Pružaoca usluge validacije tokom kojih su korišćene strukturirane metode razvoja i kontrolisano razvojno okruženje, ili;

- prilagođena hardverska i softverska rešenja razvijena od strane pouzdane strane za Pružaoca usluge validacije tokom kojih su korišćene strukturisane metode razvoja i kontrolisano razvojno okruženje, ili;

- softver otvorenog koda koji je u skladu sa bezbednosnim zahtevima i njihova adekvatnost je obezbeđena verifikacijom softvera i strukturiranim razvojem i upravljanjem životnim ciklusom.

Nabavka se sprovodi na način koji isključuje modifikaciju hardverskih i softverskih komponenti. Hardverske i softverske komponente primenjene za pružanje usluga ne smeju se koristiti u druge svrhe.

Pružalac usluge validacije sa odgovarajućim merama zaštite će sprečiti zlonamerni softver da uđe u uređaje koji se koriste u servisu sertifikacije. Pre prve upotrebe i kasnije, hardverske i softverske komponente će se redovno proveravati u potrazi za zlonamernim kodovima.

Pružalac usluge validacije će postupati sa istom pažnjom u slučaju kupovine ažuriranja programa kao pri nabavci prve verzije.
U toku instaliranja softvera i hardvera biće angažovano pouzdano, adekvatno obučeno osoblje. Pružalac usluga validacije može da instalira softver svom dobavljaču usluga samo IT opremu neophodnu u svrhu pružanja usluge.

Pružalac usluge validacije valjanosti će imati sistem kontrole verzija gde će svaka promena biti dokumentovana. Pružalac usluge validacije će primeniti procedure za otkrivanje neovlašćenih promena.

6.4.2 Kontrole upravljanja sigurnošću

Pružalac usluge validacije će implementirati procese za dokumentovanje, rad, verifikaciju, praćenje i održavanje sistema koji se koriste u usluzi, uključujući njihovu modifikaciju i dalji razvoj.
Sistem kontrole verzija će otkriti bilo koju vrstu neovlašćenih promena, unosa podataka koji utiču na sistem, zaštitni zid, rutere, programe i druge komponente koje se koriste u servisu. Instaliranjem programa koji se koristi u servisu, Pružalac usluge validacije će obezbediti da je program koji treba da se instalira ispravna verzija i da nema bilo kakvih neovlašćenih modifikacija.
Pružalac usluge validacije će redovno proveravati integritet softvera u svom sistemu koji se koristi u usluzi.

6.4.3 Sigurnosne kontrole životnog ciklusa

Pružalac usluge validacije će obezbediti zaštitu korišćenih hardverskih bezbednosnih modula tokom celog njihovog životnog ciklusa.

- Korišteni hardverski sigurnosni moduli moraju imati odgovarajuću sertifikaciju;

- po prijemu hardverskih bezbednosnih modula, proveriće se da li je obezbeđena zaštita hardverskih bezbednosnih modula od neovlašćenog pristupa tokom transporta;

- zaštita hardverskih sigurnosnih modula od neovlašćenog pristupa će biti obezbeđena tokom skladištenja;

- tokom rada, zahtevi bezbednosnog cilja hardverskih bezbednosnih modula, uputstva za upotrebu i izveštaja o sertifikaciji moraju se poštovati u svakom trenutku;

- privatni ključevi uskladišteni na hardverskim bezbednosnim modulima koji su povučeni iz upotrebe biće obrisani na takav način da je nemoguće povratiti ključeve.

- Dekomisioniranim hardverskim sigurnosnim modulima će se rukovati i odlagati u skladu sa zahtevima njihovog bezbednosnog cilja, uputstvima za upotrebu i izveštajem o sertifikaciji.

6.5 Kontrole mrežne bezbednosti

Pružalac usluge validacije će držati svoju konfiguraciju IT sistema pod strogom kontrolom i dokumentovati svaku promenu uključujući i najmanju modifikaciju, razvoj, ažuriranje softvera. Pružalac usluga validacije će primeniti odgovarajuće procedure za otkrivanje bilo kakve promene hardvera ili softvera, instalacije sistema i održavanja na IT sistemu.
Pružalac usluge validacije i integriteta svake softverske komponente pri prvom učitavanju.

Pružalac usluge validacije će primeniti odgovarajuće mere bezbednosti mreže na primer:

- svoj IT sistem će podeliti na dobro odvojene bezbednosne zone;
- odvojiće namensku mrežu za administraciju IT sistema i živu operativnu mrežu;
- treba da odvoji proizvodne sisteme za TSP usluge od sistema koji se koriste u razvoju i testiranju;
- uspostavljaće komunikaciju između različitih sistema od poverenja samo preko pouzdanih kanala koji se logički razlikuju od drugih kanala komunikacije i obezbeđuju sigurnu identifikaciju njegovih krajnjih tačaka i zaštitu podataka kanala od modifikacije ili otkrivanja;
- upravljaće IT sistemima koji se koriste za živu operativnu mrežu u zonama bezbedne mreže;
- ograničiće pristup i komunikaciju između zona na one neophodne za rad usluge;
- će onemogućiti nekorišćene protokole i naloge;
- će onemogućiti nekorišćene mrežne portove i usluge;
- pokreće samo mrežne aplikacije koje su bezuslovno neophodne za pravilan rad IT sistema;
- redovno pregledava utvrđeni skup pravila.

Pružalac usluge validacije će proći ili izvršiti skeniranje ranjivosti javnih i privatnih IP adresa:

- u roku od jedne nedelje od prijema zahteva od CA/Brovser Foruma;
- nakon bilo kakvih promena sistema ili mreže za koje CA utvrdi da su značajne;
- najmanje svaka tri (3) meseca.

6.6 Vremensko žigosanje

Pružalac usluge validacije će koristiti vremenske žigove koje daje kvalifikovani Pružalac vremenskog žiga koji je naveden na listi pouzdanih u jednoj od država članica Evropske unije za zaštitu integriteta datoteka evidencije i drugih elektronskih datoteka koje treba arhivirati.

7 Revizija usklađenosti i druge procene

Rad Pružaoca usluge validacije nadzire Ministarstvo trgovine, turizma i telekomunikacija u skladu sa propisima Evropske unije.
Ministarstvo trgovine, turizma i telekomunikacija održava inspekcije na lokaciji najmanje jednom godišnje na lokaciji pružaoca usluge validacije. Pre inspekcije na licu mesta, Pružalac usluge validacije svog poslovanja od strane eksternog revizora i šalje detaljan izveštaj o skriningu Ministarstvu trgovine, turizma i telekomunikacija u roku od 3 dana od njegovog prijema.
Tokom skrininga treba da se utvrdi da li rad Pružaoca usluga validacije ispunjava zahteve eIDAS Uredbe [1] i srodnog srpskog zakonodavstva i zahteve primenjene Politike(e) validacije i odgovarajuće izjave(e) o praksi validacije.).

Predmet i metodologija skrininga moraju biti u skladu sa sledećim normativnim dokumentima:

- UREDBA (EU) br. 910/2014 EVROPSKOG PARLAMENTA I SAVETA od 23. jula 2014. o elektronskoj identifikaciji i uslugama od poverenja za elektronske transakcije na unutrašnjem tržištu i stavljanju van snage Direktive 1999/93/EC [1];

- ETSI EN 319 403-1 Elektronski potpisi i infrastruktura (ESI); Procena usaglašenosti provajdera povereničkih usluga; Deo 1: Zahtevi za tela za ocenjivanje usaglašenosti koja procenjuju pružaoce usluga od poverenja [10]

- ETSI EN 319 401 Elektronski potpisi i infrastruktura (ESI); Opšti zahtevi politike za pružaoce usluga od poverenja [2]

- ETSI TS 119 511 Elektronski potpisi i infrastruktura (ESI); Zahtevi politike i bezbednosti za provajdere usluga od poverenja koji obezbeđuju validaciju digitalnih potpisa ili opštih podataka pomoću tehnika digitalnog potpisa [11]

Rezultat skrininga je poverljivi dokument koji je dostupan samo ovlašćenim licima.
Sertifikat o usaglašenosti izdat u skladu sa izveštajem o ocenjivanju usaglašenosti biće objavljen na veb stranici Pružaoca usluge validacije.

Pružalac usluge validacije zadržava pravo da u bilo kom trenutku, uz angažovanje nezavisnog stručnjaka, izvrši inspekciju rada Pružaoca koji posluju u skladu sa sadašnjom politikom(ama) rezervacije kako bi proverio usklađenost sa zahtevima.

7.1 Učestalost ili okolnosti procene

Pružalac usluge validacije će izvršiti ocenu usaglašenosti svake godine.

7.2 Identitet/Kvalifikacije procenjivača

Pružalac usluge validacije može obavljati interne revizije uz pomoć svojih zaposlenih koji imaju ulogu nezavisnog revizora sistema. Procenu usaglašenosti sa eIDAS i ETSI vrši organizacija koja ima kvalifikacioni mandat izdat od strane nacionalne organizacije za akreditaciju države članice EU.

7.3 Odnos procenjivača prema procenjenom entitetu

Eksternu reviziju može vršiti samo lice koje:

- je nezavisan od vlasnika, menadžmenta i poslovanja ispitanog Pružaoca usluga validacije;
- je nezavisan od ispitane organizacije, odnosno ni on ili ona, niti njegovi ili njeni najbliži rođaci nemaju nikakav radni ili poslovni odnos sa Pružaocem usluga validacije.

7.4 Teme obuhvaćene ocenjivanjem

Pregled će obuhvatiti najmanje sledeće oblasti:

- usklađenost sa zakonima koji su trenutno na snazi;
- usklađenost sa tehničkim standardima;
- usklađenost sa Politikom sertifikacije i Izjavom o praksi validacije;
- adekvatnost upotrebljenih procesa;
- dokumentacija;
- fizičko obezbeđenje;
- adekvatnost osoblja;
- IT bezbednost;
- poštovanje pravila zaštite podataka.

7.5 Radnje preduzete kao rezultat nedostatka

Nezavisni revizor će rezimirati rezultat skrininga u detaljnom izveštaju o skriningu koji pokriva testirane komponente sistema, procese i sadrži dokaze korišćene u skriningu i revizorske izjave. Utvrđene nesaglasnosti tokom ispitivanja i rokovi za njihovo otklanjanje evidentiraju se u posebnom poglavlju izveštaja.

Nezavisni revizor može evidentirati razlike i neslaganja na osnovu njihove ozbiljnosti otkriveno tokom pregleda:

- sugestije za izmene koje se opciono uzimaju u obzir;
- derogacije koje treba izbegavati obavezno.

Nezavisni revizor će bez odlaganja prijaviti uočene ozbiljne odstupanja Ministarstvu trgovine, turizma i telekomunikacija koje je ovlašćeno da preduzme potrebne mere.

Pružalac usluge validacije će pismenim putem odgovoriti na probleme koje je nezavisni revizor naveo i izvestiti o preduzetim merama za njihovo otklanjanje prilikom sledeće revizije organa.

Nezavisni revizor šalje izveštaj o proceni za svaki slučaj Ministarstvu trgovine, turizma i telekomunikacija.

7.6 Saopštavanje rezultata

Pružalac usluge validacije će objaviti zbirni izveštaj o proceni. Nije potrebno otkrivati odstupanja otkrivena tokom nezavisne procene sistema, ona se mogu tretirati kao poverljive informacije.

REFERENCE

[1] Uredba (EU) br. 910/2014 Evropskog parlamenta i Saveta od 23. jula 2014. o elektronskoj identifikaciji i uslugama poverenja za elektronske transakcije na unutrašnjem tržištu i stavljanju van snage Direktive 1999/93/EC.

[2] ETSI EN 319 401 V2.3.1 (2021-05); Elektronski potpisi i infrastruktura (ESI); Opšti zahtevi politike za pružaoce usluga od poverenja.

[3] ETSI TS 119 102-1 V1.2.1 (2018-08) Elektronski potpisi i infrastrukture (ESI); Procedure za kreiranje i validaciju AdES digitalnih potpisa; Deo 1: Kreiranje i validacija.

[4] ISO/IEC 19790:2012: Informaciona tehnologija – Tehnike bezbednosti – Zahtevi bezbednosti za kriptografske module.

[5] FIPS PUB 140-2 (2001, 25. maj): Bezbednosni zahtevi za kriptografske module.

[6] FIPS PUB 140-3 (22. mart 2019.): Bezbednosni zahtevi za kriptografske module.

[7] CEN 419 221-5; Profili zaštite za TSP kriptografske module - Deo 5: Kriptografski modul za usluge poverenja.

[8] MSZ/ISO/IEC 15408-2:2022, Informaciona tehnologija - Metode i sredstva bezbednosti - Kriterijumi za procenu IT bezbednosti .

[9] Zajednički kriterijumi za procenu bezbednosti informacionih tehnologija, deo 1 - 3.

[10] ETSI EN 319 403-1 V2.3.1 (2020-06) Elektronski potpisi i infrastrukture (ESI); Procena usaglašenosti provajdera povereničkih usluga; Deo 1: Zahtevi za tela za ocenjivanje usaglašenosti koja ocenjuju pružaoce usluga od poverenja.

[11] ETSI TS 119 511 V1.1.1 (2019-06); Elektronski potpisi i infrastruktura (ESI); Zahtevi politike i bezbednosti za provajdere usluga poverenja koji obezbeđuju dugoročno očuvanje digitalnih potpisa ili opštih podataka korišćenjem tehnika digitalnog potpisa.

[12] (Srpski) Zakon o zaštiti podataka o ličnosti („Službeni glasnik RS“ br. 87/2018).

[13] Uredba (EU) 2016/679 Evropskog parlamenta i Saveta od 27. aprila 2016. o zaštiti fizičkih lica u vezi sa obradom ličnih podataka i o slobodnom kretanju takvih podataka i stavljanju van snage Direktive 95/ 46/EC (Opšta uredba o zaštiti podataka).

[14] Zakon o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju („Službeni glasnik RS”, br. 94/2017 i 52/21).